- **Remember banks and other financial institutions will not call you and ask for personal and account information over the phone.** When in doubt, tell the caller you'll call them back and call the phone number from your account statement or other documents, rather than the caller. NEVER give out social security numbers, account information, and/or passwords over the phone to an unsolicited caller.
- **Likewise, unexpected callers who claim to be from Microsoft or other tech companies are also frauds.** If you have not contacted a company for assistance with a problem, do NOT provide personal information or install software at the request of a person claiming to be technical support. Remember, software manufacturers NEVER call users to fix viruses or apply updates.
- **If it sounds too good to be true it probably is.** Who wouldn't love to win a big prize? But if you didn't enter, you won't win. And even if you did enter and win, you wouldn't be required to pay to collect your winning. Neither would you be required to provide your bank account information.
- **Don't fall for the scare or intimidation tactics either.** Your grandson is not in jail in Mexico and needing money immediately. Your credit card isn't on the verge of being suspended. If you think either of those cases *might* be true, verify the information by trying to personally contact the person allegedly in trouble or by calling your financial institution directly. NEVER provide personal, confidential, or financial information to an unknown caller.
- **In the office, establish policies** for responding to requests such as password resets and physical access. Make sure staff members know and follow the policies.
- Last of all, **speak up if you experience something you think may have been an attempt to commit fraud or cause harm.** At the office, report the event to your help desk or security team. At home, contact local law enforcement or the Department of Justice's Office of Consumer Protection.

Social engineering is a huge threat, but we can beat it if we all do our part. Stay aware, don't share sensitive information over the phone or via email without verifying with whom you're sharing it, don't install software or visit unfamiliar websites when requested by a stranger, and don't assume that what people tell you is always the truth.

When it comes to social engineering, skepticism may be your best friend.

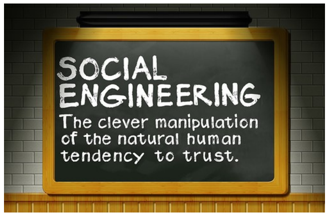
ISSO
Information Systems
Security Office
State ITSD

http://sitsd.mt.gov/MontanaInformationSecurity

Go find some other mug.
SOCIAL ENGINEERING
Verify requests for sensitive information and never share passwords with anyone.
Don't part with information if in any doubt and report all suspicious activity.
Copyright 2009 MindfulSecurity.com The Awareness Resource All Rights Reserved.

Enterprise Security Program

Social Engineering


SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

Social engineering has been used for millennia even if the phrase “social engineering” is a more recent one. One of the most infamous social engineering feats involved a city with impregnable walls, an army intent on conquering the city, a long-standing siege, and a very large horse. It’s no coincidence that malicious software that looks harmless in order to trick people into installing it and then attacks the device is called a “Trojan Horse”.

So what exactly is social engineering? In information security we define social engineering as manipulating a person to do things that he or she would not have otherwise done. It uses psychology as much as technology to achieve a goal – and sometimes doesn’t use technology at all. While it can be used in some settings for good, we generally consider social engineering to be **one of the greatest threats to security that organizations face today.**

Phishing and its phishy cousins. Some social engineering is familiar by other names. Most people know about phishing (and the variations of spear-phishing and whaling) which is a kind of social engineering that involves the use of a legitimate-looking email to trick the recipient into allowing malicious software to be installed or to provide confidential information such as account numbers and passwords.

Don’t be frightened by Scareware. This is a tool malicious actors use to frighten people into installing and/or running software. If you’ve ever seen a pop-up when surfing the internet that warns you your anti-virus is out of date, that a virus has been detected, or other problems exist on your computer, that is scareware.

Phone tactics, also known as Vishing. Using scare tactics to manipulate people can also be done over the phone. Would-be identity thieves and scam artists call people on the phone and use various scenarios to get the person to provide personal information or to give them money. For example, the caller may say that your credit card account has been compromised and in order to keep it from being suspended, you need to provide the caller with your account number and other details. Another common scam is a call about your computer being infected or in need of updates. The caller instructs the person to go to a website and download software to fix the problem.

You’re a winner! Sometimes the con is the opposite scenario – something great is in store if you’ll just do a few things or provide some information. You’ve won the lottery and all you have to do to collect is send a small processing fee. You’re the lucky recipient of an all-expenses-paid dream vacation. In order to prepare all the trip arrangements you’re asked for personal details like your birthday, address, driver’s license number, and/ or passport number.

Social engineering takes advantage of our natural inclination to want to help. The request might be in the form of a phone call asking to have a password reset for a system for which you have the authority to do so. It might be a person who knocks on the door or is standing outside an office building who says he forgot his access badge or has a meeting with someone in the building. It may be a “tech support” person who is there to fix a problem – a problem that doesn’t exist, but makes a great excuse for accessing a restricted space.

With all the methods that scam artists may use to manipulate us, it’s easy to see why so many social engineering attacks are successful and why it’s hard to defend against them.

Your best defense is to always stay alert and question anything that seems even a little bit off. Here are some more specific suggestions to help prevent you from being a victim of social engineering:

- **If you see an unaccompanied, unfamiliar person in your area, verify his identity and purpose for being there.** Do that by examining his ID, calling someone who can vouch for him, or checking with your supervisor. If he claims to work for XYZ Company and offers you a phone number, you may wish to obtain the number from an independent source.

So you're a complete stranger and you want my name, social security number and mother's maiden name? Sure, why not?
SecurityElements.com